

AI Incident Response Plan: One-Page Template for Small Teams

The AI section of your incident response plan. Keep it with your general plan, which covers everything the two share. Bracketed references are the NIST AI RMF outcomes each block supports (NIST AI 100-1).

Company: _____ Plan owner: _____ Last reviewed: _____

1. ROLES AND CONTACTS [Govern 2.1, Manage 2.4]: one name and one backup per role; phones must work if email is down

Role	Name	Backup	Phone / out-of-band contact
Incident lead (runs the response, keeps the record)			
Decision-maker (switch-off, spend, customer and regulator messages)			
AI tool owner(s) (settings, admin console, vendor contact)			
IT support / managed IT provider (revoke access, preserve logs)			
Legal counsel			
Cyber insurer or broker (policy no.)			
Bank (fraud line)			
AI vendor support / security contacts			

3. SEVEN STEPS [Manage 2.4, 4.1, 4.3]: tick and time each one

- ☐ 1. Report to the incident lead (blame-free) time _____
- ☐ 2. Stop or restrict the tool (disable, do not uninstall); use the manual fallback time _____
- ☐ 3. Preserve evidence: prompts, outputs, chat history, logs, agent actions time _____
- ☐ 4. Assess: what data, whose, how many, did output reach anyone time _____
- ☐ 5. Notify: decision-maker decides, with counsel if personal data time _____
- ☐ 6. Fix and recover: correct output, change settings, update policy time _____
- ☐ 7. Review within two weeks; update this plan time _____

5. INCIDENT RECORD [Manage 4.3]

Date found	Tool	What happened	Data involved	Who was told, when	Follow-up action, owner

2. WHAT COUNTS AS AN AI INCIDENT, AND THE FIRST MOVE [Govern 4.3, Manage 4.3]

Incident	First move
Sensitive data put into an AI tool not approved for it	Record data, tool, account, time; screenshot, do not delete yet. Stop use. Check retention/deletion and notification duties.
Wrong or harmful AI output reached a customer or a decision	Correct or withdraw it, tell recipients, check the tool's other output.
AI assistant or agent manipulated (prompt injection) or acted unapproved	Turn off the connector, revoke its tokens or keys, review what it did.
AI-enabled impersonation: cloned voice, fake video, AI-written request	Do not act. Verify on a number you already have. Call the bank if money moved. Report at ic3.gov.
Incident or outage at an AI vendor	Follow the vendor notice, rotate keys and passwords, decide whether to pause, use the manual fallback.

4. NOTIFICATION DUTIES TO CHECK [Manage 4.3]: fill in before an incident

Duty	Applies? Deadline	Owner
Customer contracts (notice clauses)		
Cyber insurance policy (notice requirement)		
State breach laws where affected people live		
HIPAA, if a covered entity or business associate		
Government contracts, if any		
Other (regulator, lender, partner)		